UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,729	04/14/2004	Mark Baugher	50325-0867	6696

29989 7590 04/10/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/824,729	BAUGHER, MARK	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/23/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 01/23/2008. In light of the applicant's amendments, the examiner hereby withdraws his previous Specification Objections, Claim Objections regarding Claims 17-19, and 35 U.S.C. 112 2nd paragraph rejections regarding Claims 1, 5, & 16. Claims 1-31 are pending and have been considered as follows.

Specification

1. The disclosure is objected to because of the following informalities:

- Page 3 paragraph 76 lines 6-7 of the amended Specification recites "a carrier wave as described hereinafter, or any other medium from which a computer can read" which should be omitted as it renders limitations with "computer readable storage medium" as non-statutory subject matter. Appropriate correction is required.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 18 & 19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 18 recites "an apparatus…with one or more stored sequences of instructions that are accessible to the processor…" which is non-statutory subject matter since it appears to be merely software modules. The examiner suggests amending that the apparatus has "a computer readable storage medium having stored thereon…"
- Claim 19 recites "a computer readable storage medium" which includes non-statutory subject matter in light of the applicant's specification as mentioned above.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 & 17-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Schuba et al. (US-6944663-B2).

Claim 1:

Schuba et al. disclose a method of preventing an attack on a network comprising,

- "receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202)") [column 3 lines 52-53];

- "wherein the request includes an accumulated work value" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];
- "if not, requiring the user to perform a quantity of work as a condition for accessing the resource" (i.e. "FIG. 2 is a flow chart illustrating the process of using a client puzzle in accordance with an embodiment of the present invention") [column 3 lines 50-52];
- "providing the user with access to the resource" (i.e. "Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];
- "determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];

- "providing the accumulated work output value to the user" (i.e. "The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 55-58].

Claims 17-19:

Schuba et al. disclose an apparatus for preventing an attack on a network comprising,

- "a processor" (i.e. "a computer system based on a microprocessor, a mainframe computer, a digital signal processor, a portable computing device, a personal organizer, a device controller, and a computational engine within an appliance") [column 3 lines 35-38];
- "one or more stored sequences of instructions that are accessible to the processor" (i.e. "The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs) and DVDs (digital versatile discs or digital video discs)") [column 3 lines 10-12];
- "receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202)") [column 3 lines 52-53];
  "wherein the request includes an accumulated work value" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];

- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];
- "if not, selectively requiring the user to perform a quantity of work as a condition for accessing the resource" (i.e. "FIG. 2 is a flow chart illustrating the process of using a client puzzle in accordance with an embodiment of the present invention") [column 3 lines 50-52];
- "providing the user with access to the resource" (i.e. "Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];
- "determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The
- system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "providing the accumulated work output value to the user" (i.e. "The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 55-58].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 20, 24, & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba et al. (US-6944663-B2).

Claims 2, 20, 24, & 28:

Schuba et al. disclose a method of preventing an attack on a network, an apparatus, and a computer-readable storage medium storing one or more sequences of instructions, as in Claims 1 & 17-19 above, further comprising,

- "determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39].

but they do not explicitly disclose,

- "wherein the request includes a prior user identity value and a current user identity value"

however, they do disclose,

- "For example, if the parameters associated with the client (id.sub.1, n, y) are stored in a database that is indexed by id.sub.1, a subsequent lookup using id.sub.2 will return

(id.sub.1, n, y) only if id.sub.1 =id.sub.2. Alternatively, if the lookup is based on client identifiers, an explicit comparison of id.sub.1 and id.sub.2 needs to be performed" [column 4 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the request includes a prior user identity value and a current user identity value," in the invention as disclosed by Schuba et al. since it would be expected that a client/user may attempt to connect more than just once and accommodations need to be made to handle the scenarios where the client is legitimate and non-legitimate as is suggested by Schuba et al.

7. Claims 3-16, 21-23, 25-27, & 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba et al. (US-6944663-B2) in view of Juels et al. (US-7197639-B1).

Claim 3:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, further comprising,

- "wherein H(i+1,x) is computed by the user as a hash chain from a non-shared user secret (x)" (i.e. "Next, the system stores (id.sub.1, n, y) at server 102 (step 208) and sends (id.sub.1, n, y) to client 106 (step 210). The system then allows client 106 to compute the preimage x, such that h(x)=y (step 212). In one embodiment of the present invention, h is a hash function, such as SHA1 or MD5, so that computing the preimage x given y requires significantly more time than computing the hash function h(x) given x") [column 3 lines 59-64];

- "wherein H(n,x)= h(H(n-1,x)" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];
- "wherein n > 0 and H(0,x) = x" (i.e. "The parameter n is used to adjust the amount of work required to compute the preimage x. For example, the parameter n can be used as a parameter to the hash function h, which indicates both the size of the hash value generated by the hash function h, as well as the number of bits of x that are used in computing h(x)") [column 4 lines 3-8];
- "wherein function h is a one-way function that is difficult to invert" (i.e. "h is a hash function, such as SHA1 or MD5, so that computing the preimage x given y requires significantly more time than computing the hash function h(x) given x") [column 3 lines 63-64];
- "receiving a current user identity value H(i,x)" (i.e. "Next, the system receives (id.sub.2, x) from the client (step 214), wherein id.sub.2 is an identifier returned by the client and x is the preimage of y computed by the client") [column 4 lines 20-22];
- "verifying that the keyless user identity value properly identifies the user only upon determining that h(H(i,x)) = H(i+1,x)" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];

but they do not disclose,

- "receiving a prior keyless user identity value H(i+1,x) in the request comprising a one-time password"

however, Juels et al. do disclose,

- "For example, after TCP-IP is established, the next higher protocol layer can demand a secret password or other form of authentication before proceeding with the execution of the server application" [column 13 lines 23-25];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving a prior keyless user identity value H(i+1,x) in the request comprising a one-time password," in the invention as disclosed by Schuba et al. since "an adversary cannot pass through this security barrier. If this were not true, then the adversary would not be limited to disabling the server 120 through session-establishing resource depletion" [column 13 lines 27-30].

Claim 4:

Schuba et al. and Juels et al. disclose a method of preventing an attack on a network, as in Claim 3 above, further comprising,

- "wherein h comprises a SHA-1 hash algorithm" (i.e. "h is a hash function, such as SHA1 or MD5, so that computing the preimage x given y requires significantly more time than computing the hash function h(x) given x") [column 3 lines 63-64].

Claim 5:

Schuba et al. and Juels et al. disclose a method of preventing an attack on a network, as in Claim 3 above, further comprising,

- "wherein n is between 10^4 and 10^6" (i.e. "The parameter n is used to adjust the amount of work required to compute the preimage x. For example, the parameter n can be used as a parameter to the hash function h, which indicates both the size of the hash value generated by the hash function h, as well as the number of bits of x that are used in computing h(x)") [column 4 lines 3-8].

Claim 6:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "determining the required work threshold value based on a then-current capacity of the resource"

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource," in the invention as disclosed by Schuba et al. or the purposes of assessing the likelihood of attack.

Claim 7:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "determining the required work threshold value based on a then-current capacity of the resource"
- "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource"
- "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource"
- "wherein the second amount of work is greater than the first amount of work"

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];
- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource" and "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource" and "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource" and "wherein the second amount of work is greater than the first amount of work," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 8:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "wherein the step of determining an amount of accumulated work output value is performed for a specified user only during a specified time period in which accumulating work is allowed for that specified user"

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the step of determining an amount of accumulated work output value is performed for a specified user only during a specified time period in which accumulating work is allowed for that specified user," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 9:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "wherein the step of determining an amount of accumulated work output value is performed for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period"

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the step of determining an amount of accumulated work output value is performed for a specified user only if the current user identity value

received from the user is not found in a list of user identity values that were previously received in a specified time period," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 10:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "digitally signing and providing a timestamp to the user with the accumulated work output value"
- "wherein the step of determining an amount of accumulated work output value is performed for a specified user"
- "only upon: receiving the timestamp is received in a subsequent request"
- "only upon: verifying the timestamp value"
- "only upon: determining that the timestamp value is within an allowed range"

however, Juels et al. do disclose,

- "This time stamp, or any other portion of seed data (SD) can be optionally authenticated with the use of a secretly computed message authentication code residing as part of the other data (OD) 530 portion of the seed data (500)" [column 19 lines 22-26];

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "digitally signing and providing a timestamp to the user with the accumulated work output value" and "wherein the step of determining an amount of accumulated work output value is performed for a specified user" and "only upon: receiving the timestamp is received in a subsequent request" and "only upon: verifying the timestamp value" and "only upon: determining that the timestamp value is within an allowed range," in the invention as disclosed by Schuba et al. since "secretly computed message authentication code residing as part of the other data" may typically be "digitally signed and time stamped" information for verification, where a client puzzle protocol is used to control graceful degradation in service.

Claim 11:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, further comprising,

- "receiving the accumulated proof of work value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39].

Claim 12:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "a prior user identity value and a current user identity value in a cookie provided by the user to the resource"
- "wherein determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user comprises determining the amount of accumulated work as 2^k * p"
- "where k is a number of bits of work previously performed by the user and p is a number of messages or packets communicated between the user and the resource"

however, Juels et al. do disclose,

- "the "client puzzle" protocol" [column 8 line 65];
- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a prior user identity value and a current user identity value in a cookie provided by the user to the resource" and "wherein determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user comprises determining the amount of accumulated work as 2^k * p" and "where k is a number of bits of work previously performed by the user and p is a

number of messages or packets communicated between the user and the resource," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 13:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "providing the accumulated work output value in a cookie sent from the resource to the user"

however, Juels et al. do disclose,

- "the "client puzzle" protocol" [column 8 line 65];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "providing the accumulated work output value in a cookie sent from the resource to the user," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 14:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but they do not disclose,

- "selectively increasing the required work threshold value for a particular user in response to congestion conditions of the resource"

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "selectively increasing the required work threshold value for a particular user in response to congestion conditions of the resource," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 15:

Schuba et al. disclose a method of preventing an attack on a network, as in Claim 1 above, further comprising,

- "wherein requiring the user to perform a quantity of work as a condition for accessing the resource comprises requiring the user to hash a message until a specified number of bits are zero" (i.e. "Next, the system stores (id.sub.1, n, y) at server 102 (step 208) and sends (id.sub.1, n, y) to client 106 (step 210). The system then allows client 106 to compute the preimage x, such that h(x)=y (step 212). In one embodiment of the present invention, h is a hash function, such as SHA1 or MD5, so that computing the preimage x given y requires significantly more time than computing the hash function h(x) given x") [column 3 lines 59-64].

Claim 16:

Schuba et al. disclose a method of preventing an attack on a network comprising,

- "receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202).") [column 3 lines 52-53];
- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];
- "providing the user with access to the resource only when the accumulated work value exceeds a required work threshold value" (i.e. "If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];

but they do not disclose,

- "wherein the request includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource"

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the request includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claims 21-23, 25-27, & 29-31:

Schuba et al. disclose an apparatus and a computer-readable storage medium storing one or more sequences of instructions, as in Claims 17-19 above, but they do not disclose,

- "determining the required work threshold value based on a then-current capacity of the resource," although Juels et al. do suggest , as recited below;
- "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource," although Juels et al. do suggest , as recited below;
- "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource," although Juels et al. do suggest , as recited below;
- "wherein the second amount of work is greater than the first amount of work," although Juels et al. do suggest , as recited below;

- "determining an amount of accumulated work output value is operable for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period," although Juels et al. do suggest , as recited below;
- "digitally signing and providing a timestamp to the user with the accumulated work output value," although Juels et al. do suggest , as recited below;
- "determining an amount of accumulated work output value is operable for a specified user only upon: receiving the timestamp is received in a subsequent request," although Juels et al. do suggest , as recited below;
- "verifying the timestamp value," although Juels et al. do suggest , as recited below;
- "determining that the timestamp value is within an allowed range," although Juels et al. do suggest , as recited below;

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];
- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];
- "inside each correct sub-puzzle solution, and comparing the time stamp (DT) with the current time to check that the (sub)puzzle has not yet expired" [column 19 lines 20-22];

- "This time stamp, or any other portion of seed data (SD) can be optionally authenticated with the use of a secretly computed message authentication code residing as part of the other data (OD) 530 portion of the seed data (500)" [column 19 lines 22-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource" and "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource" and "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource" and "wherein the second amount of work is greater than the first amount of work" and "determining an amount of accumulated work output value is operable for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period" and "digitally signing and providing a timestamp to the user with the accumulated work output value" and "determining an amount of accumulated work output value is operable for a specified user only upon: receiving the timestamp is received in a subsequent request" and "verifying the timestamp value" and "determining that the timestamp value is within an allowed range," in the invention as disclosed by Schuba et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Response to Arguments

8. Applicant's arguments filed 01/23/2008 have been fully considered but they are not persuasive.

- The applicant's argument "Schuba's process does not receive an accumulated work value in a user request. Instead, after receiving the request, the system generates a work value and ultimately provides the work value to the user. Schuba does not receive or use an accumulated work value at all" has been considered but is non-persuasive. The examiner notes that the "accumulated work value" has been interpreted as a value generated by the client/user after receiving the values and parameters to perform the computational work required in order to identify whether the client is valid. The "accumulated work value" as written in the applicant's claims is broad enough to be interpreted as such, as well as, the interpretation that it is a value included/used in subsequent work computations performed by the client/user. The examiner recommends amendments to clarify this aspect to show what appears to have been meant as a historical usage of a work value or a collection of work values over a period of time forming the "accumulated work value."
- The applicant's argument "Schuba column 3 does not describe determining an accumulated work output value based on a volume of data communicated between the resource and the user" has been considered but is non-persuasive. The examiner notes that the applicant's limitation reads as "...based on a volume of data communicated between the resource and the user..." which is interpreted as any amount of any data communicated between the resource and user. It appears the applicant may have intended this limitation to provide scope for an amount of data bits in terms of volume

that is transmitted/exchanged between the resource server and client in terms of the available bandwidth or throughput of the transmission medium affecting the amount of computational work for the client.

- The applicant's argument "Juels merely refers to "a secret password or other form of authentication" and not a "prior keyless user identify value" or a "one-time password," and the non-specific description in Juels does not suggest the specific technique that is claimed" has been considered but is non-persuasive. The examiner notes that the intention of the citation of Juels et al. was to show the receiving of user identity information with a password type of authentication (or any other form of authentication as suggested by Juels et al.) since Schuba et al. do not explicitly by themselves recite the limitation of "receiving a prior keyless user identity value H(i+1,x) in the request comprising a one-time password."
- The applicant's argument "Juels does not disclose receiving an accumulated work value in the request… Juels 9: 10- 14 says nothing about receiving an accumulated work value from a user or client, as claimed, and says nothing about receiving a value that represents work the user previously had to do. In Juels, work previously done is not accounted for at all-only new work (client puzzles of increasing size) is handed out" has been considered but is non-persuasive. The examiner notes that the provided citation in the previous office action correspondence in regards to Claim 16 was meant to provide the suggestion from Juels et al. for work that was previously required. Schuba et al. provides coverage for the limitations regarding the accumulated work value, whereas Juels et al. provides

suggestion for work that was previously required through the scalability of computations/puzzles dependent and adjusted according to previous and current conditions.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
04/08/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136